UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	
VIRGIL GRIFFITH,	:	20 Cr. 15 (PKC)
Defendant.	:	

GOVERNMENT'S MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S MOTION TO DISMISS THE INDICTMENT FOR LACK OF VENUE

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Michael Krouse
Kimberly J. Ravener
Kyle Wirshba
Assistant United States Attorneys
-Of Counsel-

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum of law in opposition to the motion of defendant Virgil Griffith to dismiss the Indictment for lack of venue pursuant to Federal Rule of Criminal Procedure 12(b)(3)(i) (the "Defense Motion"). The Indictment charges the defendant with one count of conspiring to violate the International Emergency Economic Powers Act ("IEEPA"), by providing prohibited services to the Democratic People's Republic of Korea ("DPRK" or "North Korea"). The defendant, a cryptocurrency expert, traveled to the DPRK and provided services in violation of IEEPA by, among other things, relying on his expertise to convey information to the DPRK on blockchain and cryptocurrency technologies and using these technologies to evade sanctions and launder money.

The Defense Motion argues that the Government lacks sufficient evidence to prove venue is proper in this District by a preponderance of the evidence. Specifically, the defendant highlights a March 6, 2019 email that he sent to the DPRK mission to the United Nations in Manhattan to obtain a visa to travel to the DPRK, *see* Compl. ¶ 15(d), and argues that because no records exist to confirm whether or not that email was received in the District, venue cannot be established here and the Indictment should be dismissed.

The Defense Motion fails for at least two reasons. *First*, the Indictment properly alleges that the offense occurred "in the Southern District of New York . . . and elsewhere." Dkt. No. 9, Indictment ¶ 1. No more is required to defeat a motion to dismiss. *Second*, even if the Court were to look beyond the allegations in the Indictment, the email alone constitutes proof that an act in furtherance of the conspiracy occurred in this District. Moreover, the defendant admitted to FBI agents that he sent this communication into Manhattan in order to further his plans with the DPRK.

The sufficiency of this evidence is a question for the jury, not a basis for dismissal of the Indictment. Accordingly, the Defense Motion should be denied.

RELEVANT FACTS

On November 21, 2019, Virgil Griffith was charged in a criminal Complaint with conspiring to violate IEEPA. One week later, Griffith was arrested in Los Angeles pursuant to the charge in the Complaint. On January 7, 2020, a Grand Jury sitting in this District returned an Indictment charging Griffith with conspiring to violate IEEPA.

As alleged in the Complaint, Griffith worked for Ethereum Foundation, a company that functions as an open-source platform for the development of blockchain[1] and cryptocurrency[2] technologies, including a cryptocurrency named Ethereum. In or about April 2019, Griffith traveled to the DPRK to attend and present at the "Pyongyang Blockchain and Cryptocurrency Conference" (the "DPRK Cryptocurrency Conference"). Prior to traveling to the DPRK, Griffith requested permission from the U.S. State Department to attend the DPRK Cryptocurrency Conference, but because of the North Korea Sanctions Regulations, the U.S. State Department denied the request. Ignoring this denial, Griffith unlawfully obtained a DPRK visa and traveled to the DPRK via China. *See* Compl. ¶ 5.

The evidence will show that Griffith's participation in the DPRK Cryptocurrency Conference was rooted in his intent to evade DPRK sanctions and assist the North Koreans in

[1] As described in the Complaint, a blockchain is a public, distributed electronic ledger that, among other things, records cryptocurrency transfers. The blockchain only records the movement of cryptocurrency; it does not by itself identify the parties to the transfer. As a result, the users can remain anonymous. *See* Compl. ¶ 13.

[2] As described in the Complaint, cryptocurrency is a decentralized, peer-to-peer form of electronic currency that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status. Unlike "fiat currency," such as the U.S. dollar and the Euro, cryptocurrency is not issued by any jurisdiction and functions only by agreement within the community of users of that particular currency. *See* Compl. ¶ 12.

doing the same. Griffith began developing plans to evade sanctions more than a year before he traveled to the DPRK Cryptocurrency Conference. For example, as early as on or about February 17, 2018, Griffith attempted to enlist another individual in a scheme to set up unlawful cryptocurrency equipment in the DPRK. He proposed, over an encrypted application, "[i]f you find someone [in North Korea], we'd love to make an Ethereum trip to DPRK and setup an Ethereum node."[3] When the individual questioned whether the plan made "economic sense," Griffith responded, "It does actually[.] It'll help them circumvent the current sanctions on them."

Griffith knew that facilitating sanctions evasion, and supplying his own services to help the DPRK do so, was a critical objective of the DPRK Cryptocurrency Conference. For example, on or about August 31, 2018, an individual asked Griffith, via an encrypted application, why he was willing to risk his safety to go to a conference in the DPRK. Griffith expressed that he was unafraid of the DPRK authorities, because "DPRK wouldn't want to scare away Blockchain talent that'll let them get around sanctions." In response, the individual asked, "What if they're funding their drug trade and nuclear program with crypto?" To this question, Griffith replied, "Unlikely. But they'd probably like to start doing such." In another conversation discussing the DPRK Crypto Currency Conference, on or about November 26, 2018, Griffith wrote that the DPRK's interest in cryptocurrency was "probably avoiding sanctions . . . who knows." Compl. ¶ 16(a).

Despite his understanding that the DPRK sought to utilize his expertise for sanctions evasion, and potentially to aid drug trafficking and nuclear proliferation, Griffith began preparations to travel to North Korea by early 2019. In order to attend and present at the DPRK

[3] A "node" is a computer that connects to a cryptocurrency network that is responsible for validating and relaying cryptocurrency transactions. Depending on the cryptocurrency and type of node, a computer acting as a node is often rewarded for the validation it undertakes with additional cryptocurrency, in a process called mining. An individual running a node, therefore, might also receive cryptocurrency as part of the process.

Cryptocurrency Conference, Griffith learned he had to obtain the approval of the DPRK Mission in Manhattan. Specifically, on or about February 14, 2019, Griffith received an email from a co-conspirator ("CC-1"), bearing the subject, "Applying for blockchain conference," and stating, in substance and in part:

> Because you have US passport, I already sent your data to my department in Pyongyang, the Committee for Cultural Relations with Foreign Countries. But they only can give the clearance after the first approval of our DPRK mission in NY. So, please communicate ASAP with: DPRK Mission to the U.N. E-mail: dpr.korea@verizon.net . . . Address: 820 Second Avenue, 13th Floor New York, NY 10017 USA[.] You have have [sic] to express your wish to participate in the blockchain conference from 18 to 25 April 2019, invited by the Committee for Cultural Relations with Foreign Countries. You can give the Reference/Contact person in Pyongyang: Mr. Kim Won Il, Committee for Cultural Relations with Foreign Countries. You also have to send them your passport, personal details and CV (Resume).

(Def. Mot. Ex. 1.) In response to the email from CC-1 and consistent with CC-1's instructions, Griffith sent an email to "dpr.korea@verizon.net" on or about February 18, 2019, which included the following:

> Hello to UN's DPRK Mission. I'm writing to you to request your permission to attend and speak at the blockchain conference from 18 to 25 April 2019. I have been invited by the Committee for Cultural Relations with Foreign Countries. My contact person in Pyongyang is: Mr. Kim Won Il, Committee for Cultural Relations with Foreign Countries. I attach my passport, and CV.

(*Id*.) The email address provided by CC-1, however, was incorrect; as reflected in publicly available materials, the DPRK Mission in Manhattan uses "DPRK.UN@verizon.net" as its email address. The evidence demonstrates that Griffith learned this and corrected the error. On or about March 7, 2019, Griffith forwarded his prior email to the correct email address, writing: "This is my request to visit the DPRK blockchain conference. See forwarded email below." Griffith also attached a picture of his passport and a digital link to his curriculum vitae, as CC-1 directed would be necessary to procure "the first approval of our DPRK mission in NY." On or about April 17,

2019, approximately one month after contacting the DPRK mission in New York, Griffith received a visa to visit the DPRK, *see* Compl. ¶ 15(e), a copy of which he later posted to his Twitter account.

At the DPRK Cryptocurrency Conference, in violation of the North Korean Sanctions Regulations, Griffith provided services to the DPRK attendees by: giving a presentation on topics that had been pre-approved by DPRK officials, including using cryptocurrency and blockchain technologies; supplying the conference attendees and participants—and, therefore, the DPRK—with valuable information on blockchain and cryptocurrency technologies; and relying on his expertise in discussions regarding using cryptocurrency technologies to evade sanctions and launder money. Griffith was assigned a DPRK-government handler throughout his trip to North Korea, and at times, wore a North Korean military-style uniform.

After the DPRK Cryptocurrency Conference, Griffith continued his scheme to evade sanctions. For example, on or about August 6, 2019, Griffith wrote to a contact, "I need to send 1 [unit of Ethereum] between North and South Korea." In response, the contact asked, "Isn't that violating sanctions?," to which Griffith confirmed, "it is." Compl. ¶ 16(b).

FBI agents interviewed Griffith in the United States on May 22, 2019, and November 12, 2019 about his trip to and conduct within the DPRK. *See* Compl. ¶¶ 15(a)-(k). During those interviews, Griffith acknowledged that the State Department denied his request to travel to the DPRK and admitted that he traveled anyway. In particular, Griffith told FBI agents, in sum and substance, that he had corresponded with officials at the DPRK Mission in Manhattan to facilitate his travel. Griffith explained that he had provided to the DPRK officials all of the requested documents for travel through the DPRK Mission's main email address: dprk.un@verizon.net.

Griffith said that he was required to provide scanned copies of his passport and passport photos to the DPRK Mission prior to travel and did so.[4]

ARGUMENT

I. Legal Standard

"In reviewing a motion to dismiss an indictment, the Court must take the allegations of the indictment as true." *United States v. Tucker*, No. 16 Cr. 91 (PKC), 2017 WL 3610587, at *1 (S.D.N.Y. Mar. 1, 2017) (quoting *United States v. Skelos*, 15 Cr. 317 (KMW), 2015 WL 6159326, at *2 (S.D.N.Y. Oct. 20, 2015)); *United States v. Velastegui*, 199 F.3d 590, 592 n.2 (2d Cir. 1999) ("[T]he facts alleged by the government must be taken as true" when a defendant moves dismiss an indictment). "Dismissal is an extraordinary remedy reserved only for extremely limited circumstances implicating fundamental rights." *United States v. De La Pava*, 268 F.3d 157, 165 (2d Cir. 2001) (internal quotations omitted); *see also United States v. Fields*, 592 F.2d 638, 647 (2d Cir. 1978) (noting that dismissal of an indictment is "the most drastic remedy available" and an "extreme sanction"). "Unless the government has made what can fairly be described as a full proffer of the evidence it intends to present at trial to satisfy the jurisdictional element of the offense, the sufficiency of the evidence is not appropriately addressed on a pretrial motion to dismiss an indictment." *United States v. Alfonso*, 143 F.3d 772, 776-77 (2d Cir. 1998). As a result,

[4] The Defense Motion inaccurately claims that "the government intentionally fostered the misimpression that no final charging decision had been made" in its conversations with defense counsel. (Def. Mot. 2-4.) To the contrary, the Government made no representations about whether a charging instrument had been filed. During the investigation, the Government became increasingly concerned about the risk that Griffith might flee. For example, during a consensual search of Griffith's phone, the FBI found evidence that Griffith was exploring the possibility of renouncing his United States citizenship and purchasing citizenship from another country. Following the issuance of the arrest warrant on November 21, 2019, the FBI was unable to locate Griffith for approximately one week, and therefore could not effectuate the arrest until he appeared for his scheduled flight on November 28, 2019.

"[a] pretrial motion to dismiss an indictment must not weigh the sufficiency of the evidence." *Tucker*, 2017 WL 3610587, at *2.

The proper forum for a criminal prosecution is the district in which the crime was committed. *See* U.S. Const. Art. III, § 2; *Id.* Amend. VI; Fed. R. Crim. P. 18. Where "the acts constituting the crime and the nature of the crime charged implicate more than one location," however, the Constitution "does not command a single exclusive venue." *United States v. Reed*, 773 F.2d 477, 480 (2d Cir. 1985). Instead, a defendant charged with a "continuing offense" maybe tried in any district in which some part of the offense occurred. *See, e.g.*, *United States v. Ramirez*, 420 F.3d 134, 139 (2d Cir. 2005); *United States v. Naranjo*, 14 F.3d 145, 147 (2d Cir. 1994). It is well established that in a conspiracy prosecution, venue is proper "in any district in which an overt act in furtherance of the conspiracy was committed." *United States v. Tzolov*, 642 F.3d 314, 319-20 (2d Cir. 2011). Indeed, proof of an overt act by any of the co-conspirators in a district will support venue there as to all of them. *United States v. Ramirez-Amaya*, 812 F.2d 813, 816 (2d Cir. 1987). "Thus, a defendant need not himself have ever been physically present in a district for a conspiracy charge against him to be venued there." *United States v. Rommy*, 506 F.3d 108, 119-20 (2d Cir. 2007); *see also United States v. Tang Yuk*, 885 F.3d 57, 69 (2d Cir. 2018). For example, venue is appropriate where a defendant located outside the District transmits a communication into the District that furthers the charged conspiracy. *See, e.g.*, *Tang Yuk*, 885 F.3d at 71 (citing *Rommy*); *see also United States v. Gomez*, 751 F. App'x 63, 69 (2d Cir. 2018).

At trial, because venue is not an element of the crime, the Government must prove venue by a preponderance of the evidence, rather than beyond a reasonable doubt. *United States v. Davis*, 698 F.3d 179, 185 (2d Cir. 2012); *see also Rommy*, 506 F.3d at 119 (collecting cases). "Where venue is challenged on a pre-trial motion to dismiss," however, "the Government's burden is

limited to showing that the indictment alleges facts sufficient to support venue." *United States v. Peterson*, 357 F. Supp. 2d 748, 751 (S.D.N.Y. 2005). It is well established in this District that "[t]he Government need only allege that criminal conduct occurred within the venue, even if phrased broadly and without a specific address or other information, in order to satisfy its burden with regard to pleading venue." *United States v. Ohle*, 678 F. Supp. 2d 215, 231 (S.D.N.Y. 2010) (internal quotation marks and citation omitted). Accordingly, "it is sufficient to defeat defendant's venue motion that the indictment alleges in [each count] that the conduct occurred 'in the Southern District of New York and elsewhere,'" *United States v. Elcock*, No. 07 Cr. 582 (CM), 2008 WL 123842, at *3 (S.D.N.Y. Jan. 10, 2008); *see also Ohle*, 678 F. Supp. 2d at 231 (same); *United States v. Szur*, No. 97 Cr. 108 (JGK), 1998 WL 132942, at *9 (S.D.N.Y. Mar. 20, 1998) (same). "Whether such acts alleged in the Indictment in fact occurred . . . is appropriately left for trial. . . ." *Szur*, 1998 WL 132942, at *9.

II. Discussion

A. Venue Is Properly Alleged in the Indictment

The Defense Motion should be rejected because, as the defendant concedes, the Indictment clearly alleges that the charged crimes occurred "the Southern District of New York, the [DPRK], and elsewhere." (Def. Mot. 4.) "As to venue, the Indictment is therefore facially valid." *United States v. Teman*, No. 19 Cr. 696 (PAE), 2019 WL 6998634, at *1 (S.D.N.Y. Dec. 29, 2019); *see also, e.g.*, *Elcock*, 2008 WL 123842, at *3. Moreover, "[e]xcept where the Government has given a full proffer of the evidence it intends to present at trial, there is no basis for a court to look beyond a facial charge so as to dismiss an indictment, whether for insufficient evidence or improper venue." *Teman*, 2019 WL 6998634, at *1. The Government has not made such a proffer in this case and its investigation is very much ongoing. Accordingly, the defendant cannot achieve the extraordinary sanction of dismissing the Indictment at this phase of the case.

B. The Defendant's Venue Challenge Fails on the Merits

Even if the Court looks beyond the venue allegations in the Indictment, which it need not do, this submission and the Complaint allege facts sufficient to establish venue in this District by a preponderance of the evidence at trial.

CC-1 wrote to the defendant that in order to attend and present at the DPRK Cryptocurrency Conference, the DPRK "only can give the clearance after the first approval of our DPRK mission in NY." The defendant complied. He sent an email to the DPRK Mission in Manhattan, after learning that the DPRK Mission was located in Manhattan and used a Manhattan area code phone number. Within approximately one month, the defendant received a visa to travel to the DPRK. Later, during a May 22, 2019 FBI interview, Griffith confirmed that he understood that his travel to the DPRK was approved by the DPRK Mission, and that he communicated with the DPRK Mission, specifically acknowledging its location in New York.

The Government can establish its burden at trial based on that evidence alone. In a conspiracy case, a communication from outside the District to a party in the District "can establish venue within the district provided the conspirator uses the [communication] to further the conspiracy." *Rommy*, 506 F.3d at 122; *see also Tang Yuk*, 885 F.3d at 71; *United States v. Friedman*, 998 F.2d 53, 57 (2d Cir. 1993). The defendant's email to the DPRK Mission in Manhattan, sent at the direction of his co-conspirator, was a critical step in his quest to unlawfully provide services to the DPRK. As CC-1 explained, the defendant would not have been able to travel to the DPRK Cryptocurrency Conference without approval from the DPRK Mission. Sending the email to request the DPRK Mission's approval was therefore plainly an "overt act in furtherance of the conspiracy [that] occurred" in this District, irrespective of whether the defendant or any of his co-conspirators were ever physically present here. *Naranjo*, 14 F.3d at 147 ("The defendant need not have been present in the district, as long as an overt act in furtherance of the

conspiracy occurred there."); *see also United States v. Lange*, 834 F.3d 58, 70 (2d Cir. 2016) ("An overt act is any act performed by *any* conspirator for the purpose of accomplishing the objectives of the conspiracy. . . . This includes not just acts by co-conspirators but also acts that the conspirators cause others to take that materially furthered the ends of the conspiracy." (quoting *Tzolov*, 642 F.3d at 319-20).

The defendant contends that the Indictment should be dismissed because there are no records confirming that his email to the DPRK Mission was in fact received in Manhattan. The argument is a challenge to the sufficiency of the evidence, which is an issue for the jury to decide at trial. *See Alfonso*, 143 F.3d at 776 (finding error where "the district court looked beyond the face of the indictment and drew inferences as to the proof that would be introduced by the government at trial" on a motion to dismiss).

Even as a sufficiency challenge, the defendant's argument lacks merit. First, particularly in light of the applicable preponderance standard, the absence of IP address records related to the defendant's email to the Manhattan office of the DPRK Mission does not foreclose a finding of venue in this District.

Second, the defendant presents no IP-address data related to the routing of his email. At trial, the pertinent question will be the location to which the defendant sent the communication and not, as the defendant now suggests, the location from which a DPRK Mission employee accessed the account. The defendant has not even presented location data from the time period in which the defendant sent the email. He instead relies on account login data from between April 18, 2019 and October 30, 2019, a period commencing more than a month after the defendant sent the message to the DPRK Mission on or about March 6, 2019. The defendant's data sheds no light on the time between when he sent the email and when DPRK approved his travel on or before

April 17, 2019, the date listed on his DPRK visa. As a result, the data upon which the defendant relies in support of the motion has limited relevance to the case and is of no utility in pressing a motion to dismiss the Indictment.

Third, the defendant concedes that records produced in discovery "show" that the DPRK Mission email address "was accessed from servers purportedly located in this District 215 times" between April 18, 2019 and October 30, 2019. (Def. Mot. 5.) That figure represents more than one-third of all of the available logins. (*See id.*) Therefore, even the evidence relied upon by the defendant shows a pattern of the DPRK Mission's email account being regularly accessed from the District, consistent with the face of the email, the defendant's admissions to the FBI, and the physical location of the DPRK Mission in the Southern District of New York.

Fourth, the IP address data cited by the defendant, which relates to logins to the DPRK Mission email account, does not necessarily reflect the location where email would be received, read, or acted upon. There is no dispute that the DPRK Mission is physically located in Manhattan, and the trial evidence will show that, by the terms of their visas, DPRK Mission personnel are not permitted to travel more than 25 miles away from Columbus Circle, in Manhattan, New York. The IP login data, by contrast, reflects the computer or server that directly connected to the Oath email servers that host the DPRK Mission's email account, which is not necessarily the computer that the end user used to access the account and receive the email. For example, if the end user logged into a virtual private network ("VPN") from the DPRK Mission's Manhattan office before logging into the Oath email account, the Oath logs would reflect the VPN's IP address, not the end user's IP address. The effect is that login data through a VPN connection would not match the user's true physical location. The limited utility of this login data is suggested by the defendant's own motion, which claims that the data shows the DPRK Mission email address "was accessed from

servers in Ashburn, Virginia; Portland, Oregon; Manhattan, New York; Dublin, Ireland; and Baku, Azerbaijan." (Def. Mot. 5.) It is exceedingly unlikely that such a pattern reflects a user's access points, particularly personnel affiliated with the DPRK Mission, who are not permitted to travel to Ashburn, Virginia or Portland, Oregon, by the terms of their visas. The geographic range of IP addresses reflected in the records proffered by the defendant do not alter that reality; if anything, they are more likely to be technological red herrings, created through the use of sophisticated means that may not show one's true location. For all of these reasons, the defendant's arguments, even if entertained at this premature stage of the proceedings, fail to establish a lack of venue in this case.

Lastly, although the defendant does not appear to argue for a transfer of venue to the Central District of California, where he concedes that venue would lie, any motion to transfer venue would similarly be meritless. Transfer of venue is mandatory when "the defendant cannot obtain a fair and impartial trial" and permissible "for the convenience of the parties, any victim, and the witnesses, and in the interest of justice." Fed. R. Crim. P. 21. Where, as here, the defendant lived abroad prior to his arrest and the witnesses are not concentrated in any particular location, transfer would be inappropriate. *See United States v. Miller*, 808 F.3d 607, 623 (2d Cir. 2015) (noting a failure to make a motion for change of venue but dismissing the possibility of success because witnesses hailed from many different locations and because the defendant "had been living in Ireland for over a year").

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court deny the defendant's motion to dismiss the Indictment for lack of venue in its entirety.

DATED: New York, New York
June 10, 2018

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney
Southern District of New York

By: __/s/ _____

Michael Krouse
Kimberly J. Ravener
Kyle Wirshba
Assistant United States Attorneys
Tel: (212) 637-2279/2358/2493